Department of Defense

MANUAL

NUMBER 5200.45
April 2, 2013

USD(I)

SUBJECT: Instructions for Developing Security Classification Guides

References: See Enclosure 1

1. PURPOSE. This Manual reissues DoD 5200.1-H (Reference (a)) as a DoD Manual in accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (b)) and DoD Instruction (DoDI) 5200.01 (Reference (c)) to provide guidance for the development of security classification guidance pursuant to section 2.2 of Executive Order (E.O.) 13526 (Reference (d)), part 2001.15 of title 32, Code of Federal Regulations (CFR) (Reference (e)), and DoD Manual 5200.01 (Reference (f)).

2. APPLICABILITY. This Manual applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

3. DEFINITIONS. See Glossary.

4. RESPONSIBILITIES

a. Under Secretary of Defense for Intelligence (USD(I)). The USD(I) shall, in accordance with Reference (c), oversee the DoD Information Security Program, which includes the development, distribution, maintenance, revision, and cancellation of security classification guides.

b. Original Classification Authorities (OCAs). OCAs, as required by Reference (f), shall:

(1) Issue and disseminate security classification guidance for each system, plan, program, project, or mission involving classified information under their jurisdiction.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
02 APR 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Instructions for Developing Security Classification Guides	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense,Under Secretary of Defense for Intelligence (USD(I),1400 Defense Pentagon,Washington,DC,20301-1400**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**54**	

(2) Review security classification guidance issued under their authority once every 5 years to ensure currency and accuracy, or sooner when necessitated by significant changes in policy or in the system, plan, program, project, or mission, and update the guides as required.

(3) Revise, whenever necessary for effective derivative classification, the security classification guides issued under their authority.

(4) Provide copies of any security classification guides issued under their authority as required by Enclosure 6 of Volume 1of Reference (f).

(5) Cancel security classification guides when all information the guide specified as classified has been declassified, or when a new classification guide incorporates the classified information covered by the old guide and there is no reasonable likelihood that any information not incorporated by the new guide shall be the subject of derivative classification.

(6) Coordinate, pursuant to part 1045 of title 10, CFR (Reference (g)), with the Department of Energy (DOE), Office of Classification, through the Deputy Assistant Secretary of Defense for Nuclear Matters (DASD(NM)), whenever they develop or revise security classification guides with Restricted Data (RD) or Formerly Restricted Data (FRD) information.

5. PROCEDURES. See Enclosure 2.

6. RELEASABILITY. UNLIMITED. This Manual is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This Manual:

a. Is effective April 2, 2013.

b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DoDI 5025.01 (Reference (h)). If not, it will expire effective April 2, 2023 and be removed from the DoD Issuances Website.

Michael G. Vickers
Under Secretary of Defense for Intelligence

TABLE OF CONTENTS

TABLES

FIGURES

ENCLOSURE 1

REFERENCES

(a) DoD 5200.1-H, "Department of Defense Handbook for Writing Security Classification Guidance," November 1999 (hereby cancelled)
(b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
(c) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008, as amended
(d) Executive Order 13526, "Classified National Security Information," December 29, 2009
(e) Part 2001 of title 32, Code of Federal Regulations
(f) DoD Manual 5200.01, "DoD Information Security Program," February 24, 2012, as amended
(g) Part 1045 of title 10, Code of Federal Regulations
(h) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012
(i) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
(j) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
(k) Sections 2014 and 2162, et seq., of title 42, United States Code (also known as "The Atomic Energy Act of 1954, as amended")
(l) DoD Instruction 5210.02, "Access to and Dissemination of Restricted Data and Formerly Restricted Data," June 3, 2011
(m) DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012
(n) National Security Decision Directive 189, "National Policy on the Transfer of Scientific, Technical and Engineering Information," September 21, 1985
(o) Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, "Fundamental Research," May 24, 2010[1]
(p) DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008, as amended

[1] Available from the Office of the Assistant Secretary of Defense for Research and Engineering.

ENCLOSURE 2

PROCEDURES

1. INTRODUCTION

a. Classification management procedures call for the timely issuance of comprehensive guidance regarding classification of information concerning any system, plan, program, project, or mission under the jurisdiction of the OCA, the unauthorized disclosure of which reasonably could be expected to cause damage to national security. Precise classification guidance is prerequisite to effective and efficient information security and assures that security resources are expended to protect only that which truly warrants protection in the interests of national security. Reference (d) and its implementing guidance, Reference (e), provide general requirements and standards concerning the issuance of security classification guides while Reference (f) provides DoD guidance on development, promulgation, distribution, maintenance, and cancellation of security classification guides.

b. Information is classified, in accordance with guidance in References (d), (e), and (f), to provide an appropriate level of protection. Therefore, it is essential that a classification guide identify the specific items of information and the levels of protection required, as well as the time periods for which protection must be provided.

c. A classification guide will be issued as early as practical in the life cycle of the classified system, plan, program, project, or mission. The requirements of Reference (f) regarding classification, declassification, downgrading, marking, and security classification guides should be reviewed and understood in preparation for writing a security classification guide.

d. DoD information that does not, individually or in compilation, require classification, must still be reviewed in accordance with DoDD 5230.09 (Reference (i)), prior to any release to the public. In addition, such information must also be reviewed for compliance with the provisions of DoDI 8550.01 (Reference (j)), prior to its placement on any publicly accessible Internet site. Information that does not require classification may nevertheless be exempt from release to the public or have other restrictions applied when released to other U.S. Government agencies.

e. RD and FRD are unique categories of classified information defined by section 2014 of title 42, United States Code (U.S.C.) (also known and hereinafter referred to as "The Atomic Energy Act of 1954, as amended" (Reference (k))) and for which program guidance is provided in Reference (g). Guides containing RD or FRD topics must be coordinated with DOE, through the DASD(NM); see part 1045.37(c) of Reference (g) and DoDI 5210.02 (Reference (l)) for further guidance. Note also that RD and FRD are never automatically declassified and such information must not include declassification instructions (however, see Reference (f) for further guidance when RD or FRD and national security information (NSI) are co-mingled).

f. Where applicable, guides should be marked with the appropriate distribution statement required by DoDI 5230.24 (Reference (m)). Additionally, as needed, guides should provide

direction to users to ensure assignment of the appropriate distribution statement to documents containing information addressed by the guide's content. This direction can be provided in Section 1 of the guide or in the remarks column of the classification table, as appropriate.

2. CLASSIFICATION AND DECLASSIFICATION

a. Classification Decisions

(1) Information is classified either originally or derivatively. Original classification occurs when information is developed that inherently meets the criteria for classification in accordance with Reference (d), or for nuclear weapon information, in accordance with Reference (g). Original classification cannot reasonably be derived from a previous classification decision still in force involving, in substance, the same or closely related information. A security classification guide is the written record of an original classification decision or series of decisions regarding a system, plan, program, project, or mission. Derivative classification occurs when the information already known to be classified is paraphrased, restated, or incorporated in a new document or form and the newly developed material is marked consistent with the classification markings that apply to the source information.

(2) Classification may be applied only to information that is owned by, produced by or for, or is under the control of the U. S. Government. Unclassified information that has been officially released may not be originally classified. Declassified information that has been officially released may be reclassified only in very limited cases. For a complete review of those exceptions see the guidance in References (d), (e), and (f).

(3) Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security and it pertains to one or more of the categories specified in subsections 1.4(a) through 1.4(h) of Reference (d):

(a) Military plans, weapon systems, or operations (subsection 1.4(a));

(b) Foreign government information (subsection 1.4(b));

(c) Intelligence activities (including covert action), intelligence sources or methods, or cryptology (subsection 1.4(c));

(d) Foreign relations or foreign activities of the United States, including confidential sources (subsection 1.4(d));

(e) Scientific, technological, or economic matters relating to the national security (subsection 1.4(e));

(f) U.S. Government programs for safeguarding nuclear materials or facilities (subsection 1.4(f));

(g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security (subsection 1.4(g)); or

(h) The development, production, or use of weapons of mass destruction (subsection 1.4(h)).

(4) For classification and declassification of nuclear weapon information (i.e., RD and FRD), see References (g) and (l).

(5) Pursuant to National Security Decision Directive 189 (Reference (n)), fundamental research not clearly related to the national security shall, to the maximum extent possible, remain unrestricted. However, when control is required for national security reasons, classification is the appropriate mechanism. Refer to Reference (n) and Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum (Reference (o)) for additional guidance.

(6) Although information developed by contractors under an independent research and development (IR&D) effort typically does not qualify for classification, it is possible for classified information to be generated by IR&D efforts. This may occur when contractors use properly classified information in their IR&D efforts to explore technological advancements and state-of-the-art improvements. Information that is generated by or results from an IR&D effort and is derived from properly classified information requires derivative classification in accordance with Reference (d). Classification guides developed in accordance with this Manual can be used by contractors as a source of up-to-date classification guidance for information used in or generated by their IR&D efforts. Recognition of such use by developers of classification guides, particularly those addressing leading edge or breakthrough technology, can help to ensure that information related to national security is consistently protected.

(7) An OCA determines whether specific information should be classified, using the steps shown in Appendix 1 to this enclosure. These steps may be laid out as a series of questions, as identified in subparagraphs 2.a.(7)(a) through 2.a.(7)(e). OCAs should review the following questions throughout the process:

(a) Is the information owned by, produced by or for, or under the control of the U. S. Government? If the answer to this question is no, the information cannot be classified.

(b) Does the information fall within one or more of the categories of information identified in sections 1.4(a) through 1.4(h) of Reference (d) or, for nuclear information, meet the criteria in Reference (g)? If the answer to this question is no, the information cannot be classified. If the answer is yes, then the next question applies.

(c) Is there a reasonable possibility that the information can be protected from unauthorized disclosure? If the answer is no, the information cannot be classified. If the answer is yes, then the next question applies.

(d) Can the unauthorized disclosure of the information reasonably be expected to cause identifiable or describable damage to the national security? If the answer is no, the information cannot be classified. If the answer is yes, then the question in subparagraph 2.a.(7)(e) applies.

(e) What is the level of damage (i.e., damage, serious damage, or exceptionally grave damage) to the national security expected in the event of an unauthorized disclosure of the information? If the answer to this question is damage, classify the information "Confidential." If the answer is serious damage, classify it "Secret." If the answer is exceptionally grave damage, classify the information "Top Secret."

(f) Where there is significant doubt about the need to classify information, it shall not be classified. If there is significant doubt about the appropriate level of classification, the information shall be classified at the lower level.

b. When to Declassify. The declassification decision determines how long the information will be protected (i.e., the duration of classification) and is as important as the original classification determination. Information is to be declassified as soon as it no longer meets the requirements for classification. When an item of information is **originally** classified, the OCA shall establish a specific date or event for declassification of the information based upon its national security sensitivity. The OCA must specify one of the following options, selecting, whenever possible, the option that will result in the shortest duration of classification:

(1) A date or independently verifiable event less than 10 years from the date of original classification.

(2) A date 10 years from the date of original classification.

(3) A date or independently verifiable event greater than 10 and less than 25 years from the date of original classification.

(4) A date 25 years from the date of original classification.

(5) "50X1-HUM," designating a duration of up to 75 years, when classifying information that is clearly and demonstrably expected to reveal the identity of a confidential human source or a human intelligence (HUMINT) source.

(6) "50X2-WMD," designating a duration of up to 75 years, when classifying information that is clearly and demonstrably expected to reveal key design concepts of weapons of mass destruction.

(7) "25X_" (where "_" is a number 1 through 9) with a date or event, designating a duration of up to 50 years when classifying information that clearly falls within an exemption from automatic declassification at 25 years that has previously been approved by the Interagency Security Classification Appeals Panel (ISACP). See Enclosure 5 of Volume 1 of Reference (f) for further guidance on use of exemptions before citing this duration.

c. Downgrading. References (d) and (e) allow OCAs to specify applicable downgrading instructions at predetermined points in time or when specified events occur. OCAs are encouraged to use these provisions to specify dates or events for downgrading when the lower classification level will provide adequate protection.

d. Exemptions. Exemptions from automatic declassification approved in accordance with References (d), (e), and (f) may be incorporated into classification guides provided the ISCAP is notified in advance of the intent to take such action and the information remains in active use. Consult Volume 1 of Reference (f) for further guidance on exemptions and the notification process.

3. PLAN OF ACTION FOR WRITING CLASSIFICATION GUIDES

a. Step 1 - Consider Related Current Guidance

(1) Before writing a security classification guide, it is necessary to find out what, if any, classification guidance exists that is applicable to items of information concerning the system, plan, program, project, or mission for which the new classification guide is being constructed. In addition to guides for specific efforts or missions, in some fields or subject areas guides that apply to a broad spectrum of activities, sometimes referred to as "umbrella guides," have been issued. Any existing guidance should be considered carefully. Uniformity and consistency in the exercise of classification authority, especially in the form of a security classification guide, are essential. Beware of conflicts between the guide being developed and any previously approved guide(s).

(2) Defense Technical Information Center (DTIC) provides an on-line index of most of the guides issued within DoD. Many of the listed guides are available from DTIC. Always check the DTIC listing (http://www.dtic.mil/dtic/registration/; registration required) but be aware that some classification guides are deemed too sensitive to be included. In addition, there may be other classification guides issued along functional lines by activities outside DoD that could have a bearing on the effort. Seek the advice of those who have knowledge of classification in the subject area under consideration or in closely related fields. The local information security manager or information security specialist may also be a valuable source of advice and assistance. DASD(NM) or the DOE Office of Classification can provide assistance in the classification of nuclear weapon information. The DoD Special Access Program Central Office may be able to provide assistance to special access programs. The Acquisition Security Database (https://asdb.strikenet.navy.smil.mil) is another source that can be consulted for information on related guidance. The database can be used to identify critical program information for research, development, and acquisition programs, projects, or systems with potentially similar technology and information. Additionally, USD(I)/Security Directorate may be able to be of assistance in identifying sensitive classification guides when other sources have be exhausted; forward requests through the security chain of command.

(3) Once potentially similar information is identified, follow up as needed to understand whether the information is the same or different and, if the same, to ensure consistent, horizontal classification of the information. When there is a conflict in classification guidance between the guide being developed and a previously approved guide, there is a risk of unauthorized disclosure. Thus, it is important to understand and resolve such differences. Conflicts shall be resolved and the resulting guidance approved by the responsible OCAs. In cases where the data is similar but not the same, include an explanation of the differences in the data and their classification levels in the guide so that the users can clearly understand those differences and protect the information appropriately.

b. Step 2 - Determine the State-of-the-Art Status. Reasonable classification determinations cannot be made in the scientific and technical field without analysis of what has been accomplished, what is being attempted, and by whom. Use Appendix 3 to help with that analysis. Make use of scientific and information services. Consult technical and intelligence specialists. Obtain assistance available from any proper source. Learn about the state of the art, the state of development, attainment in the field of work, and what is known and openly published about it, including:

(1) The known or published status (foreign and domestic).

(2) The known but unpublished (possibly classified) status in the United States.

(3) The known but unpublished status in friendly and unfriendly countries.

(4) The extent of foreign knowledge of the unpublished status in the United States.

c. Step 3 - Identify National Advantage. The guide's subject matter must be reviewed as a totality. Appendix 2 can also help with that review. Decide what the system, plan, program, project, or mission does or seeks to accomplish that will result in a net national advantage. Cover all the benefits, direct and indirect, accruing or expected to accrue to the United States. In the final analysis, the decision to classify will be related to one or more of the following factors that produce, directly or indirectly, the actual or expected net national advantage:

(1) Fact of interest by the U.S. Government in the particular effort as a whole or in specific parts that are being considered or emphasized.

(2) Fact of possession by the United States.

(3) Capabilities of the resulting product in terms of quality, quantity, and location.

(4) Performance, including operational performance, as it relates to capabilities.

(5) Vulnerabilities, weaknesses, countermeasures, and counter-countermeasures.

(6) Uniqueness – exclusive U.S. knowledge.

(7) Lead time, related to state of the art.

(8) Surprise, related to possession and capability to use.

(9) Specifications – may be indicative of goals, aims, or achievements.

(10) Manufacturing technology.

(11) Associations with other data or activities.

d. Step 4 - Make Initial Classification Determination. Conducting the analysis outlined in paragraphs 3.b. and 3.c. of this section will help identify the net national advantage, and hence, what requires classification to protect that advantage. Although at this stage of the guide's preparation the focus is primarily on information relating to the overall effort, consideration must be given to some of the more specific information or data that covers performance capabilities and possible vulnerabilities and weaknesses. Appendix 3 to this enclosure has been designed to help in that consideration.

(1) Before trying to identify specific items of information that require classification, some sense of what information about the system, plan, program, project, or mission needs protection is required. Use an engineering approach or view of the effort to group information about the effort into large categories and then consider each category in turn. One or more of the large categories may be able to be eliminated from further consideration with relative ease (i.e., none of the information in the category qualifies for or requires classification). A work breakdown structure or system architecture may help identify the categories. After the large categories are identified, they can be repetitively broken into smaller and smaller pieces until specific elements of information are identified.

(2) Additionally, be aware that the information that needs protection may change as a system, plan, program, project or mission progresses through its life-cycle. What needs to be classified in the early stages of a system, plan, program, project or mission (e.g., during research and development) may differ from that which requires classification in other life-cycle phases (e.g., system development, production, operations or execution). The effort must be regularly reevaluated to determine which information requires classification and the classification guidance updated as appropriate.

(3) Once the information that needs to be protected has been identified, do not forget to look at all the related processes (e.g., manufacturing, logistics, budgeting) to ensure the information is protected throughout execution of those processes (e.g., do the budget estimates need to be classified? does shipment of the end-item to certain locations reveal classified data?).

e. Step 5 - Identify Specific Items of Information That Require Classification

(1) The core of a classification guide is the identification of the specific items or elements of information warranting security protection. Regardless of the size or complexity of the subject matter of the guide, or the level at which the classification guide is issued, there are certain identifiable features of the information that create or contribute to actual or expected

national security advantage. There also may be certain items of information that need to be protected to prevent or make it more difficult for hostile forces to develop or apply timely and effective countermeasures. The challenge is to identify and state those special features or critical items of information and to decide how and why they are related to the net national advantage.

(a) Some additional questions and items of information relating to the identification of classifiable details are laid out in Appendices 3 and 4 of this enclosure and in Enclosure 3.

(b) Statements or descriptions identifying the items of information to be classified must be clear and specific so as to minimize the probability of error by those who will use the classification guide.

(2) Research, development and acquisition projects and programs should consider critical program information identified in accordance with DoDI 5200.39 (Reference (p)) when writing the security classification guide to ensure that it is properly protected.

(3) It is also important that the level of classification to be applied to each item of information identified in the guide be specified precisely and clearly. Broad guidance such as "U-S," meaning "Unclassified to Secret," does not provide sufficient instruction to users of the guide, unless the exact circumstances under which each level of classification should be applied are delineated. The exact circumstances must be supplied in amplifying comments, for example, "Unclassified (U) when X is not revealed; Confidential (C) when X is revealed; Secret (S) when X and Y are revealed." Failure to provide such guidance will result in users of the guide (derivative classifiers) making their own interpretations that may, or may not, be consistent with the intent. Additionally, failure to provide such guidance may lead to over or under classification of information, which impacts information sharing and can add additional cost to the security program or result in inadequate protection or unauthorized disclosure.

(4) Information that has been officially released to the public may not be classified or reclassified, except in very limited cases; see Reference (f) for detailed guidance. This restriction does not apply to unauthorized releases, such as "leaks"; such information does not require reclassification because it remains classified until declassified by the OCA.

f. Step 6 - Determine the Duration of Classification

(1) Equally important to a determination to classify is the decision on how long the classification should remain in effect. (Remember no determination is required for RD and FRD as they are not subject to the automatic declassification provisions of Reference (d).) Factors that may influence this decision include:

(a) At the conceptual stage of a new effort there may be good reason to classify more information about the effort than will be necessary in later phases. Some information loses its sensitivity and importance in terms of creating or contributing to the national advantage over time. Information must continuously be evaluated to determine the need for continued classification.

(b) At certain stages in production or deployment, it may not be practical or possible to protect certain items of information from disclosure. It is also possible that design improvements may have eliminated exploitable vulnerabilities.

(c) Once a decision is made to release information to the public, it cannot remain classified.

(2) With these factors in mind, and considering the provisions of paragraph 2.b. of this enclosure, proceed with the determination of the appropriate declassification instructions for each item of classified information.

(3) Always consider the possibility of providing for downgrading of the classification that is assigned. Future downgrading is an option that is always open when information is originally classified at the "S" or "TS" levels. Consider it carefully in every instance and provide for downgrading at fixed future points in time or upon a specified event occurring when the damage that is expected to result from an unauthorized disclosure will be reduced to a level prescribed for lower classification.

g. Step 7 - Write the Guide. Once the specific items of information that warrant security classification have been identified, it is finally time to start writing the security classification guide. Use clear, precise language and statements to describe which items of information require classification.

(1) While there is no mandatory DoD-wide format for security classification guides, first consider using the format described in Enclosure 4 of this Manual.

(2) Security classification guides should be issued as documents within the OSD or DoD Component policy or regulatory structure (e.g., instructions, manuals, regulations) only in exceptional cases. Typically, the issuing office coordinates the guide with other subject matter experts and potential users prior to approval by the OCA and promulgation by the issuing office. This process facilitates timely update of the guide, as required by References (d) and (e).

(3) Comply with these administrative requirements:

(a) Place the most significant words of the guide's title first, for example, "FA-5B Aircraft Security Classification Guide."

(b) Identify the OCA who personally approved the guide in writing and has program or supervisory responsibility over the information addressed in the guide as well as the office of primary responsibility (OPR) that can be contacted for clarification or additional information.

(c) Specify, clearly and concisely, the reason(s) for classification, the level of classification, and a declassification instruction(s) for each item to be classified. A table format is recommended for identifying this information as well as any downgrading instructions and other needed comments and instructions. While the format used throughout this Manual is the recommended format, the format can vary for clarity or to best suit the needs of the system, plan,

program, project, or mission. The Appendix to Enclosure 4 of this Manual illustrates some format variations.

(d) Classify the guide if required by its contents. If the guide does not require classification, it must be marked and protected as FOR OFFICIAL USE ONLY (FOUO). Security classification guides shall not be released to the public.

(4) Ensure that the security classification guide:

(a) Precisely states the specific information elements to be protected. Use clear, precise language or statements to describe which items of information require classification. It is also advisable to include items that are designated as controlled unclassified information (CUI) (e.g., FOUO) or that are unclassified, when that will assure users of the guide that this information is, in fact, CUI or unclassified and was not inadvertently omitted.

(b) Identifies the classification levels ("TS," "S," or "C") and any additional dissemination control marking or special handling caveats such as RD, FRD, Releasable To (REL TO), or Not Releasable to Foreign Nationals (NOFORN), that may apply to each element of information. When it will serve a useful purpose or reassure the user, specify that the information is "U" (Unclassified) or cite the specific CUI control (such as FOUO).

(c) Identifies the reason for classification, using the number of the applicable subsection of section 1.4 of Reference (d).

(d) Specifies the duration of classification for each element of information, except for information that qualifies as RD or FRD. As RD and FRD are not subject to the automatic declassification requirements of Reference (d), no declassification instruction should be entered for RD or FRD information unless co-mingled with NSI. Alternatively, when not co-mingled with NSI, "Excluded from automatic downgrading/declassification" may be cited in the "Declassify On" column for clarity. When co-mingled, see Volume 2 of Reference (f) for further guidance.

(e) States any downgrading action that is to occur, and when such action is to take place (date or event).

(f) Includes amplifying comments whenever appropriate to explain the exact application of classification.

(5) Provide any additional guidance required for effective use of the guide. Use the general instructions in section 1 of the guide to address general topics (e.g., foreign disclosure considerations, public affairs guidance, dissemination, and reproduction information) that provide overall guidance for the users.

Appendixes

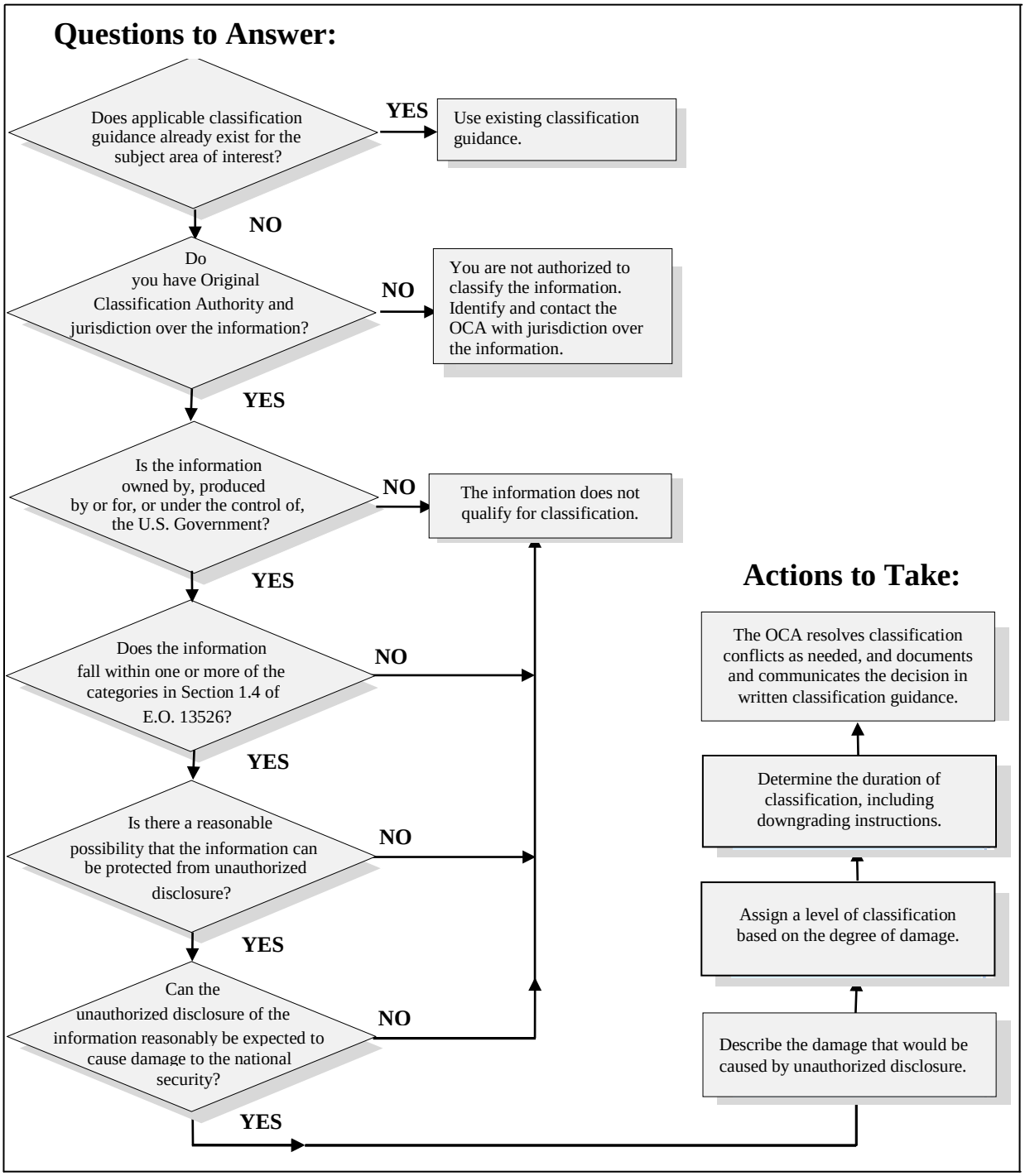
1. Original Classification Process
2. Classification Factors

3. Classifying Details
4. Specific Items of Information to Consider

APPENDIX 1 TO ENCLOSURE 2

ORIGINAL CLASSIFICATION PROCESS

Figure 1. Original Classification Process Flow Chart



APPENDIX 2 TO ENCLOSURE 2

CLASSIFICATION FACTORS

The questions, answers, and follow-up actions shown in Figure 2 are provided to assist in systematically determining whether certain broad aspects of an effort warrant security classification. Users are cautioned that the outcomes specified in the flow chart are not absolute; judgment must be applied in all cases. Additionally, when using Figure 2 it may be necessary to consider the questions for both the overall effort and, at a high level, for the individual technologies used. For example, the fact that a new weapon system (the overall effort) is being developed may be public knowledge and therefore not classifiable, but aspects of specific technologies used in the weapon system may warrant protection and, therefore, be classifiable. If the resulting determination is that the information is classifiable, see Appendix 3 to Enclosure 2 for guidance on determining which specific details of the effort warrant classification.

Figure 2. Classification Factors Flow Chart

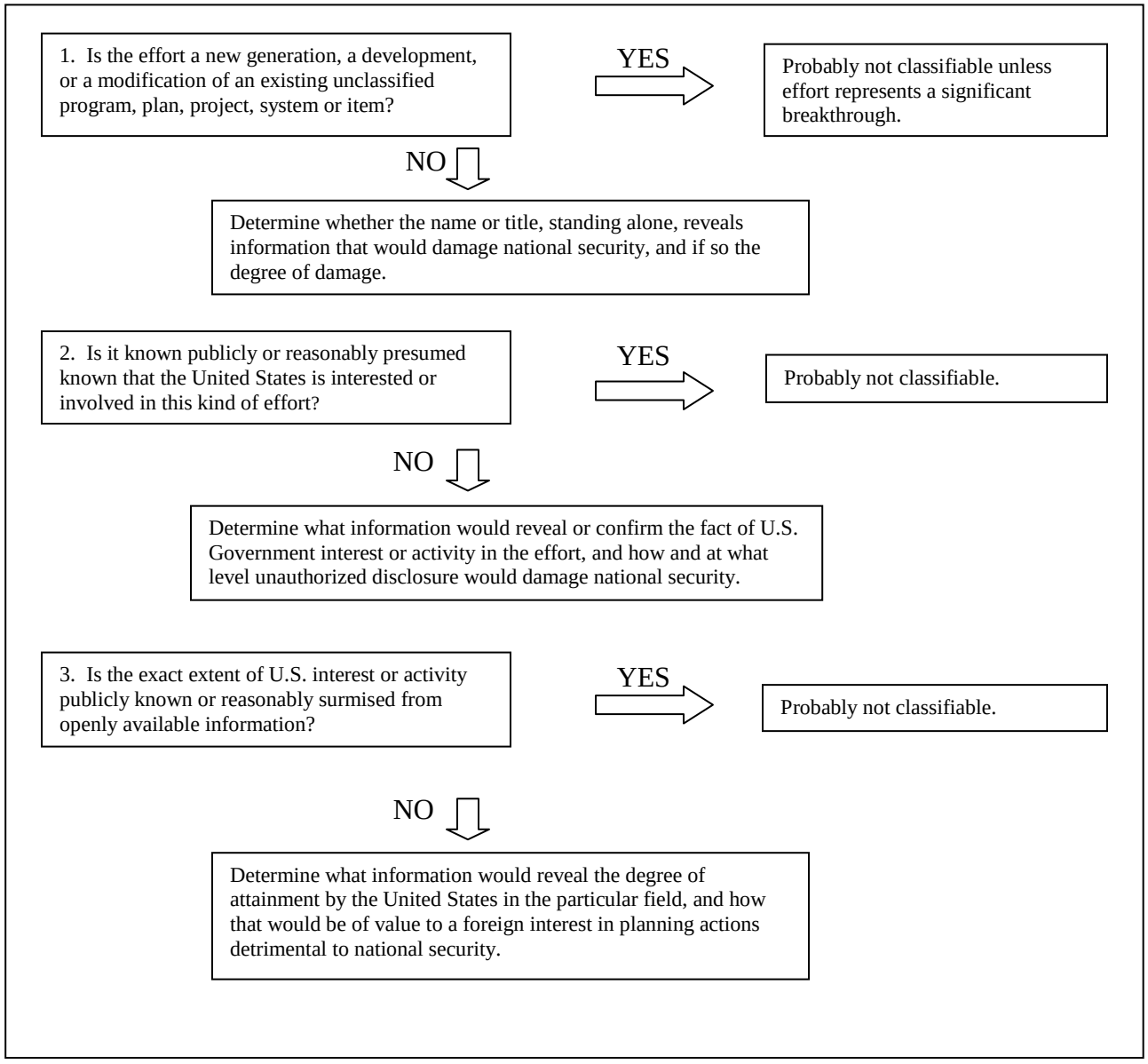
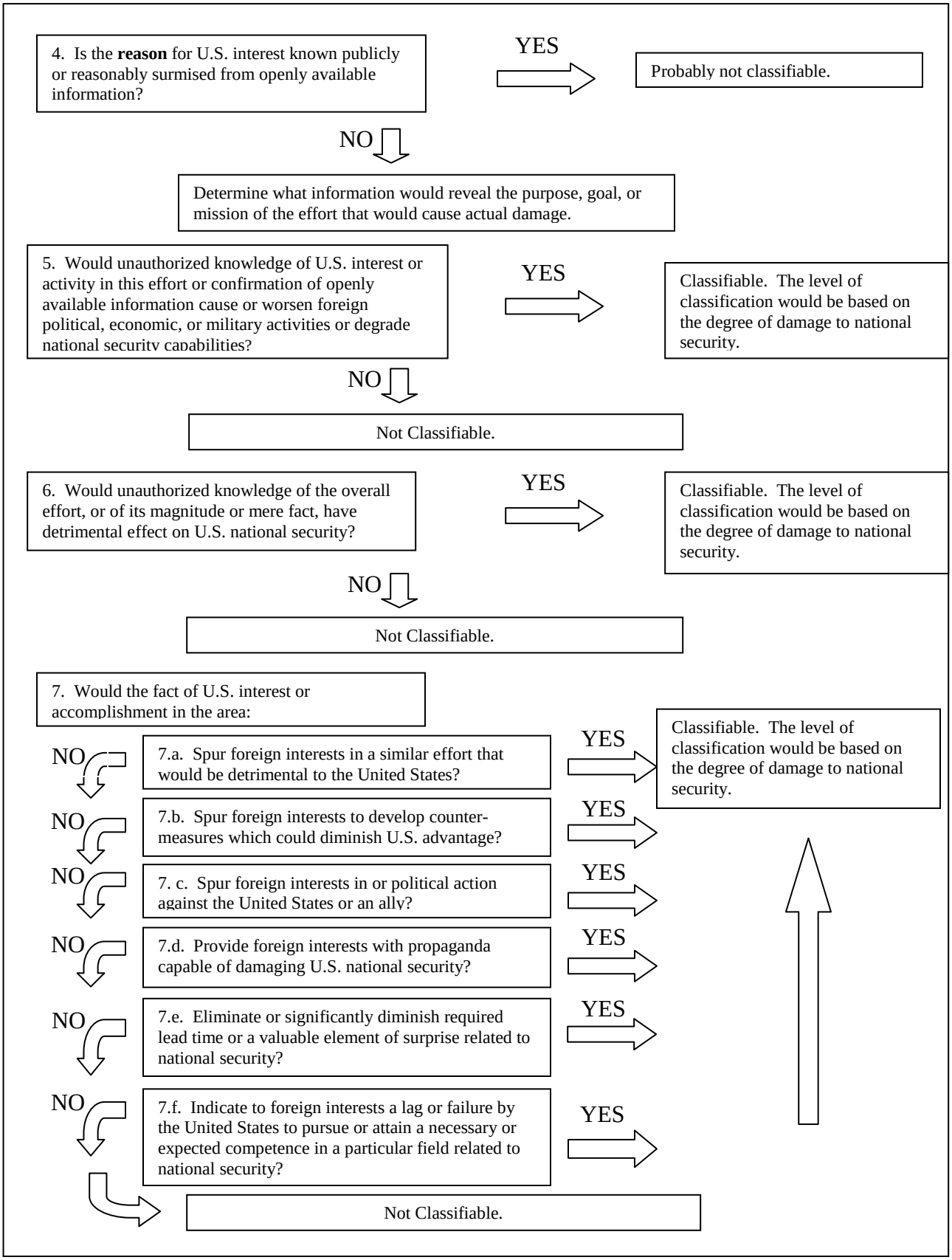


Figure 2. Classification Factors Flow Chart, Continued



APPENDIX 3 TO ENCLOSURE 2

CLASSIFYING DETAILS

1. OVERVIEW. Having considered the factors involved in making classification determinations concerning the overall effort, the next step is to consider the classification of certain specific details of the effort. While the questions in sections 2 – 11 of this appendix are not presented in any order of priority, providing answers to them will help to systematically bound and refine the scope of the analysis needed to determine which items warrant protection through security classification. When doing the analysis, also consider the items listed in Tables 1 – 5 in Appendix 4 to Enclosure 2; they may help to identify specific details that should be addressed.

2. PERFORMANCE OR CAPABILITY

a. What will this do (actual or planned) that is better, faster, or cheaper (in terms of all types of resources) than anything like it?

b. How does this degree or kind of performance contribute to or create a national security advantage? How much of an advantage?

c. How long can this data be protected? What is the advantage?

d. How would knowledge of these performance details help an enemy or damage the success of the effort?

e. Would statement of a particular degree of attained performance or capability be of value to hostile intelligence in assessing U.S. capabilities? Would such a statement spur a foreign nation to similar effort, or to develop or plan countermeasures?

f. What, if any, counterintelligence implication does system performance have? Is the performance measure of a system something that should be made known as a show of force or should it be protected so as to not reveal system weaknesses?

3. UNIQUENESS

a. What information pertaining to this effort is known or believed to be the exclusive knowledge of the United States?

b. Is it known or reasonable to believe that other nations have achieved a comparable degree of success or attainment?

c. What information, if disclosed, would result in or assist other nations in developing a

similar item or arriving at a similar level of achievement?

d. In what way or ways does the uniqueness of this item contribute to a national security advantage?

e. In what way or ways has the end product of this effort or any of its parts been modified, developed, or applied so as to be unique to this kind of effort? How unique is this?

f. Is the method of adaptation or application of the end product or any of its parts the source of the uniqueness and a national security advantage? In what way or ways? Is it in itself a unique adaptation of application in this kind of effort?

4. TECHNOLOGICAL LEAD TIME

a. How long did it take to reach this level of performance or achievement?

b. How much time and effort have been expended? Was this a special concerted effort or only a gradual developmental type of activity?

c. If all or some of the details involved in reaching this stage of development or achievement were known, how much sooner could this goal have been reached? Which details would contribute materially to a shortening of the time for reaching this goal? Can these details be protected? For how long?

d. Have other nations reached this level of development or achievement?

e. Do other nations know how far the United States has advanced in this kind of effort?

f. Would knowledge of this degree of development or achievement spur a foreign nation to accelerate its efforts to diminish our lead in this field? What details of knowledge would be likely to cause such acceleration?

g. How important, in terms of anticipated results, is the lead-time gained?

h. What national security advantage actually results from this lead-time?

i. How long is it practical to believe that this lead-time will represent an actual advantage?

j. How long is it practical to expect to be able to protect this lead-time?

5. SURPRISE

a. Do other nations know about this level of development or achievement?

b. Will operational use of the end item of this effort give the U.S. an immediate advantage that would be less or lost if the achievement of this particular goal were known?

c. What is the nature of the advantage resulting from surprise use of this end item?

d. When will this element of surprise be lost?

6. VULNERABILITIES AND WEAKNESSES

a. What are the weak spots in this effort that make it vulnerable to failure? What is the rate or effect of this failure?

b. How will the failure of the effort in whole or in part affect the national security advantage expected upon completion of this effort, or use of the resulting end item?

c. What elements of this effort are subject to countermeasures?

d. How would knowledge of these vulnerable elements assist in planning or carrying out countermeasures?

e. Can information concerning these weak or vulnerable elements be protected from unauthorized disclosure or are they inherent in the system?

f. Can these weaknesses or vulnerabilities be exploited to reduce or defeat the success of this effort? How could this be done?

g. Are the counter-countermeasures obvious, special, unique, unknown to outsiders or other nations?

h. How would knowledge of these counter-countermeasures assist in carrying out or planning new countering efforts?

i. Would knowledge of specific performance capabilities assist in developing or applying specific countermeasures? How? What would be the effect on the expected national security advantage?

7. SPECIFICATIONS

a. What would details of specification reveal?

(1) A special or unusual interest that contributes to the resulting or expected national security advantage?

(2) Special or unique compositions that contribute to the resulting or expected national security advantage?

(3) Special or unique levels of performance that are indicative of a classifiable level of achievement or goal?

(4) Special or unique use of certain materials that reveals or suggests the source of a national security advantage?

(5) Special or unique size, weight, or shape that contributes to the resulting or expected national security advantage?

b. Are any specification details contributory to the resulting or expected national security advantage? How?

c. Can details of specifications be protected? For how long?

8. CRITICAL ELEMENTS

a. What are the things that really make this effort work?

b. Which of these critical elements contribute to the resulting or expected national security advantage? How? To what extent?

c. Are these critical elements the source of weakness or vulnerability to countermeasures?

d. What details of information pertaining to these critical elements disclose or reveal the national security advantage, weakness or vulnerability?

e. Can details of information pertaining to these critical elements be protected by classification? For how long?

9. MANUFACTURING TECHNOLOGY

a. What manufacturing methods, techniques, or modes of operation were developed to meet the requirements of this effort?

b. Which of these manufacturing innovations are unique to this effort or this product? Are they generally known or suspected?

c. Are these manufacturing innovations essential to successful production of the product?

d. What kind of lead-time results from these innovations?

10. ASSOCIATIONS

a. Are there any associations between this effort and others that raise classification questions?

b. Are there associations between information in this effort and already publicly available (unclassified) information that raise classification problems?

c. Are there associations with specific personnel, commands, companies, or other programs that are sensitive and should be protected or that may reveal classified information?

d. Is it necessary or possible to classify items of information in this effort because their association with other unclassified or classified information would diminish or result in the loss of a national security advantage?

11. PROTECTABILITY

a. Is it possible to effectively protect the information from unauthorized disclosure by classifying it? For how long?

b. What alternative means can be used to ensure protection from unauthorized disclosure? Are they as effective as classification?

APPENDIX 4 TO ENCLOSURE 2

SPECIFIC ITEMS OF INFORMATION TO CONSIDER

Tables 1 through 6 present categories of data and lists of items of information that could disclose present or future strategic or tactical capabilities and vulnerabilities and that should be considered when preparing classification guidance. The items are listed alphabetically within each table and are intended to help the user identify specific items of information that qualify for and warrant protection by classification.

Table 1. Performance and Capability Related Data

Accuracy
Alert time
Altitude
  Maximum
  Optimum
Ballistics
  Initial
  Terminal
Control
Countermeasures (proven, unproven)
  Counter-countermeasures
  Decoys
  Electronic
  Penetration aids
  Shield materials
Depth/height (also of burst)
  Maximum
  Optimum
Duration (flight)
Effectiveness
Frequencies (bands, specific, command, operating, infrared, microwave, radio, communications security (COMSEC))
Heating
Impulse
Intercept
Lethality/critical effects
Lift
Limitations
Maneuverability
Military strength
  Actual
  Planned, predicted, anticipated
Miss distance
	Noise figure
	Operational readiness time cycle
	Payload
	Penetration
	Range (range scales)
	Rate of fire
	Reaction time
	Reliability/failure rate data
	Resolution
	Sensitivity
	Sequence of events
	Signature characteristics
	  Acceptance
	  Analysis
	  Distinguishment
	  Identification
	Speed/velocity
	  Acceleration/deceleration
	  Cruise
	  Intercept
	  Landing
	  Maximum
	  Minimum
	  Optimum
	Stability
	Target data
	  Details
	  Identification
	  Illumination
	  Impact predicted
	  Preliminary
	  Priority
	  Range determination
	Thresholds
	Thrust
	Toxicity

Table 2. Specifications Related Data (Detailed, Basic)

Balance
Burn rate
Capacity (system)
Center of gravity
Codes
Composition
Configuration/contour
Consumption
Energy requirements
  Specific
  Total
Filter
Fineness
Grain configuration
Hardness, degree
Input data
	Loading/loads
	Mass factor (propellant)
	Moment of inertia
	On-station time
	Output data
	Payload
	Power requirements
	Purity
	Size, weight, shape
	Stability (static, dynamic)
	Strength of members, frames
	Stress
	Thickness
	Type

Table 3. Vulnerability Related Data

Countermeasures/counter-countermeasures
Dynamic pressure (supersonic)
Electromagnetic pulse (radiation)
Ground or air shock
Jamming
	Signature characteristics
	  Acoustic
	  Electrical
	  Infrared
	  Magnetic
	  Pressure
	  Radar
	  Static overpressure

Table 4. Procurement, Production, and Logistics Related Data

Completion date or dates Numbers Dispersion (numbers per unit of force) On-hand stockpile Planned or programmed (total scheduled) Rate of delivery or production Requirements Spares	Progress/schedules (milestones) Stock density Supply plans and status Tactical deployment Timelines Logistical resupply Maintenance and repair cycle

Table 5. Operations Related Data

Countdown time Deployment data Environment Location Numbers available Objectives Mission or program Specific or general Test, broad or detailed Plans Command and control (including reaction time)	Results Analysis, conclusions, reports Sequence of events Staging techniques Statement/concept Tactical Build-up Units per force Activation and capability dates Personnel

Table 6. Testing Related Data

Dates Location Objectives General Specific Output (raw; analyzed) Plans	Required equipment or personnel Results Analysis, conclusions, reports Schedule

ENCLOSURE 3

CLASSIFYING SPECIFIC TYPES OF INFORMATION

1. CLASSIFYING HARDWARE ITEMS

a. Basic Considerations. An item of hardware may convey information that is as sensitive as the words printed upon a piece of paper. Hardware items may be classified if they reveal information or information can be obtained from them. Some basic considerations are:

(1) An item of hardware does not necessarily need to be classified simply because it is part of a classified product or effort.

(2) Unclassified off-the-shelf items, unless modified in some particular way to make them perform differently, can never be classified even though they constitute a critical element, become an integral part of a classified end product, or produce a properly classified effect. However, the association of otherwise unclassified hardware with a particular effort or product may reveal something classified about that effort or product. Common integrated circuits that control frequencies are notable examples. In such cases, it is the association with the effort or product that reveals the classified information, not the circuits themselves. Decisions regarding what aspect of the system to classify may be difficult but are necessary to delineate for users of the guide what information requires protection.

(3) Frequently, classified information pertaining to a hardware item can be restricted to the documentation associated with the item.

(4) Unusual, unique, or peculiar uses or modifications of ordinarily available unclassified materials or hardware may create a classifiable item of information. In another instance, just using a particular material in a particular effort might reveal a classifiable research or development interest. In such cases, it is especially important to accurately identify the classified information to determine whether it is the hardware or material that reveals classified information or the association of uses of the hardware with a particular effort that reveals such information.

(5) At some stage in a production effort, production and engineering plans are drawn. Usually a family-tree type diagram is prepared to assist in determining what components, parts, and materials will be required. This diagram provides a good basis for determining where and when classified information will be involved in the production effort.

(6) Another usual step in production engineering is the development of drawings for all the individual elements that go into the final product. These drawings show design data, functions, and specifications, all of which are closely tied with items of information that may be classified. From these drawings it is possible to determine exactly which elements of the final product will reveal classified information. It is also possible to determine associations that may

reveal classified information. This is a prime opportunity to identify and isolate classification requirements.

b. User Considerations. Pay attention to who will be using the classification guide.

(1) Usually management and staff supervisory personnel need to have a fairly broad knowledge of classification requirements. Farther down the line, however, foremen and workers usually need to know only which hardware items are classified, the appropriate levels of classification, and which items are unclassified. Therefore, as soon as possible in the production planning process, make a listing of all classified hardware items according to part number or other identifier, and when necessary for understanding, a listing of unclassified items. Such a listing will be valuable to procurement and logistics (e.g., shipping, handling, and storage) personnel. The listing should preferably be unclassified and should be reviewed carefully to ensure that the listing itself does not reveal classified information.

(2) When planning a production line, careful attention is needed to delay as long as possible the insertion of classified hardware items.

(3) Test equipment rarely embodies classified information. When such equipment is used to test tolerances, specifications, performance, and other details that are classified, the equipment would still be unclassified unless it was calibrated or set in such a way as to reveal the classified information pertaining to the item being tested. This is one example of a situation where it may be possible to limit the classified information to the documentation involved and to the test operator's personal knowledge, precluding the necessity for classifying the test equipment itself.

2. CLASSIFYING MILITARY OPERATIONS INFORMATION

a. General. The security classification of military operations information (defined in the Glossary) is subject to the considerations described in Enclosure 2 and its appendices. While there are no hard and fast rules for the classification of military operations information and while each Military Service and Combatant Command may require a unique approach to operations security (OPSEC), there are basic concepts that can be applied.

b. Military Operations Classification Considerations

(1) Successful military operations depend largely upon the DoD's ability to assess correctly the capability and intention of enemy forces at each stage of the operation while concealing its own capabilities and intentions, and to communicate effective battle plans and orders throughout our forces. Classifiable information may include:

(a) The number, type, location, and strengths of opposing units.

(b) The capabilities and vulnerabilities of weapons in enemy hands, and how the enemy normally applies the weapons.

(c) The morale and physical condition of the enemy force.

(2) In considering classification guidance for military operations, there may be good reason to classify more information about the operations in the beginning than will be necessary later. Certain elements of information such as troop movements may no longer require the same level of protection after a certain date or event. When this point is reached, downgrading or declassification should be pursued.

(3) Table 7 provides examples of information relating to military operations that may warrant classification. Actual durations must be specified as required by Reference (f) and summarized in paragraph 2.b of Enclosure 2 of this Manual.

Table 7. Examples of Information Related to Military Operations

DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY

TOPIC	CLASS	REASON	DECLASSIFY ON	REMARKS
1. Overall operational plans		1.4(a)	Date or event within 25 years	
2. System operational deployment or employment		1.4(a)	Declassify upon completion of deployment or employment	
3. Initial operational capability (IOC) date		1.4(a)	Declassify upon attainment of IOC date	
4. Planned location of operational units		1.4(a)	Declassify upon arrival on site	
5. Equipage dates, readiness dates, operational employment dates		1.4(a)	Declassify upon attainment of the milestone events	
6. Total manpower or personnel requirements for total operational force		1.4(a)	Declassify upon completion of operation	
7. Coordinates of selected operational sites		1.4(a)	Declassify upon site termination	Downgrade to "C" after site activation
8. Specific operational performance data that relates to the effectiveness of the control of forces and data on specific vulnerabilities and weaknesses		1.4(a)	Date or event within 25 years	
9. Existing OPSEC and COMSEC measures		1.4(a)	Date or event within 25 years	
10. Target characteristics		1.4(a)	Date or event within 25 years	

3. CLASSIFYING INTELLIGENCE INFORMATION

a. Intelligence Classification Considerations. Producers of intelligence must avoid over classification and be wary of applying so much security that they are unable to provide a useful product to their consumers. An intelligence product should be classified only when its disclosure

could reasonably be expected to cause some degree of damage to national security. Subparagraphs 3.a.(1) through 3.a.(10) lists some basic considerations, but they are not all-inclusive.

(1) In general, resource information should not be classified unless it reveals some aspect of the intelligence mission, and its revelation would jeopardize the effectiveness of a particular function. An example of classifiable resource information is the intelligence contingency fund.

(2) Intelligence concerning foreign weapons systems is typically classified based on what is generally known about a particular system or its components. Normally, the less that is known publicly about a particular system or component the higher its level of classification.

(3) Intelligence identifying a sensitive source or method should always be classified, as should be the evaluation of the particular source or method.

(4) Intelligence that does not identify or reveal a sensitive source or method is usually not classified unless the information contains other classified information such as intelligence activities including intelligence plans, policies, or operations.

(5) Intelligence that reveals the identity of a conventional source or method normally does not require classification. However, if the information is communicated to the DoD by a foreign government, whether under a formal government-to-government agreement or simply with the understanding that the information is provided in confidence, the information must be protected at the level and for the length of time agreed to by the U.S. Government and the foreign government. If the information is obtained from a foreign government without any agreement or restrictions, the classification, if any, should be based solely on the content of the information provided.

(6) Intelligence that reveals known and possible enemy capabilities to collect and exploit information from a given or similar operation should be classified. This would include enemy intelligence collection and analysis capabilities, efforts, and successes.

(7) An intelligence estimate is normally classified since it is likely to contain sensitive sources or methods, and/or raw or evaluated intelligence.

(8) An intelligence requirement should be classified when it reveals what is not known, what is necessary to know, and why. Moreover, the requirement may recommend a sensitive source or method, other military intelligence required, or contain technical and operational characteristics of classified weapons systems.

(9) The classification of relationships with foreign intelligence organizations is related to the considerations in subparagraphs 3.a.(9)(a) through 3.a.(9)(d):

(a) Normally, the fact of broad, U.S. general intelligence cooperation with foreign countries or groups of countries with which the United States maintains formal military alliances or agreements (e.g., the North Atlantic Treaty Organization (NATO)) is not classified.

(b) The fact of intelligence cooperation between the United States and a specific governmental component in an allied country or general description of the nature of intelligence cooperation between the United States and any allied country may be classified. The fact of ongoing intelligence cooperation between the United States and specifically named countries or their governmental components with which the United States is **not** allied should **always** be classified. Such classification is applied to U. S. intelligence activities pursuant to subsections 1.4(c) and (d) of Reference (d) to preclude the harm to national security that would clearly result should the cooperation be revealed through unauthorized disclosure.

(c) Details of any intelligence exchange agreements should also be classified. Additionally, the fact of the mere existence of such an agreement should be classified in accordance with paragraph 3.a.(9)(b), as the agreement is evidence of on-going intelligence cooperation.

(d) The identities of foreign governmental or military personnel who provide intelligence under such agreements or liaison relationships may be classified in accordance with the instructions of the foreign government or in the national security interest of the United States.

(10) Defense users must respect security classification assigned to intelligence received from non-Defense sources. Original classification authorities within the Intelligence Community normally consider information in the categories listed in subparagraphs 3.a.(10)(a) through 3.a.(10)(ae) to be classified. The level of classification depends upon the degree of identifiable harm to national security that would reasonably be expected to occur from unauthorized disclosure.

(a) Cryptologic information (including cryptologic sources and methods), cryptographic information, signals intelligence, imagery intelligence, electronics intelligence, telemetry intelligence, and electronic warfare.

(b) Counterintelligence. Information that reveals counterintelligence activities, investigations, or operations, identities of undercover personnel or units, methods of operations, and analytical techniques for the interpretation of intelligence data is classified.

(c) Intelligence special access programs.

(d) Information that identifies clandestine organizations, agents, sources, or methods.

(e) Information on personnel under official or nonofficial cover, or revelation of a cover arrangement.

(f) Covertly obtained intelligence reports and the derivative information that would divulge intelligence sources or methods.

(g) Methods or procedures used to acquire, produce, or support intelligence activities.

(h) Intelligence organizational structure, size, installations, security, objectives, and budget.

(i) Information that would divulge intelligence interests, value, or extent of knowledge on a subject.

(j) Training provided to or by an intelligence organization that would indicate its capability or identify personnel.

(k) Intelligence personnel recruiting, hiring, training, assignment, and evaluation policies.

(l) Information that could lead to foreign political, economic, or military action against the United States or its allies.

(m) Events leading to international tension that would affect U.S. foreign policy.

(n) Diplomatic or economic activities affecting national security or international security negotiations.

(o) Information affecting U.S. plans to meet diplomatic contingencies affecting national security.

(p) Non-attributable activities conducted abroad in support of U.S. foreign policy.

(q) U.S. surreptitious collection in a foreign nation that would affect relations with the country.

(r) Covert relationships with international organizations or foreign governments.

(s) Information related to political or economic instabilities in a foreign country threatening American lives and installations.

(t) Information divulging U.S. intelligence and assessment capabilities.

(u) Defense plans and capabilities of the United States and its allies that could enable a foreign entity to develop countermeasures.

(v) Information disclosing U.S. systems and weapons capabilities or deployment.

(w) Information on research, development, and engineering that enables the United States to achieve or maintain a significant national advantage in the area of national security.

(x) Information on technical systems for collection and production of intelligence.

(y) U.S. nuclear programs and facilities.

(z) Foreign nuclear programs, facilities, and intentions.

(aa) Contractual relationships that reveal the specific interest and expertise of an intelligence organization.

(ab) Information that could place an individual in jeopardy.

(ac) Information on secret writing when it relates to specific chemicals, reagents, developing, microdots, or steganography.

(ad) U.S. military space programs.

(ae) U.S. cyber capabilities.

(af) Information on weapons of mass destruction, whether U.S. or foreign.

b. Intelligence Declassification Considerations. Normally intelligence will remain classified for a longer duration than other types of classified information, but still only as long as is necessary to protect a certain source or method. The guidance for determining the duration of classification in paragraphs 2.b and 3.f of Enclosure 2 is applicable to all information, including intelligence.

c. Classification Guide Illustrations. The considerations for classifying details (see Appendixes 3 and 4 to Enclosure 2) and recommended format for a security classification guide (see Enclosure 4) are applicable to the development of an intelligence security classification guide. In addition, Table 8 is provided as an example of security classification guidance that might be applied to a HUMINT effort. Notice that the conditions upon which each classification within a range of classification applies must be differentiated as discussed in Enclosure 2, paragraph 3.e.(2). Care should also be taken to differentiate between a range of classification (e.g., "C - TS" meaning Confidential through Top Secret) and alternative classifications (e.g., "C, TS" meaning Confidential or Top Secret). In every case, it is imperative that criteria for each of the differing levels be included in the Remarks column. For example, "C if xxx," "S when yyy."

Table 8. HUMINT Classification Guidance Example

CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY

TOPIC	CLASS	REASON	DECLASSIFY ON	REMARKS
1. Biographic information taken exclusively from open source, where no intelligence connection is shown	U	not applicable (N/A)	N/A	
2. Positive identification of an individual as source to a U.S. intelligence agency	S – TS	1.4(c)	50X1-HUM	"S" if identified as a potential source "TS" if identified as an actual source
3. Identity of a target installation	C, TS	1.4(c)	25 years from origination	"C" when **not** linked to a specific collection operation "TS" when linked to a specific collection operation
4. Identity of a target personality	S – TS	1.4(c)	50X1-HUM	"S" when **not** linked to a specific collection operation "TS" when linked to an actual source or specific collection operation
5. Interest in specific events for collection exploitation, including specific areas of technology	S	1.4(c)	25 years from origination	
6. Names of collection agency case officers in conjunction with a specific collection operation	C	1.4(c)	25 years from origination	
7. Information on collection agency HUMINT policy plans, plans, methods, or accomplishments	S	1.4(c)	25 years from origination	50X1-HUM if information can clearly and demonstrably be expected to reveal identity of confidential human source or HUMINT source

4. CLASSIFYING FOREIGN RELATIONS INFORMATION

a. General. The Department of State is the agency primarily responsible for the development and execution of the foreign policy of the United States, and thus is also the primary agency responsible for the security classification of foreign relations information. Most DoD classification determinations in the area of foreign relations will be derivative in nature. However, there will be instances where DoD projects and programs involve foreign relations information for which security classification guidance must be developed.

b. Foreign Relations Classification Considerations. Examples of the types of information or material involving foreign relations that warrant classification consideration include:

(1) All information or material recommending or revealing U.S. Government positions or options in a negotiation with a foreign government or group of governments, or comments on the merits of foreign government positions in such negotiations.

(2) All information or material that comments on the quality, character, or attitude of a serving foreign government official, whether elected or appointed, and regardless of whether the comment is favorable or critical. Illustrations of the types of information covered in this category are records revealing:

(a) A foreign official speaking in a highly critical manner of his own government's policy.

(b) A foreign official suggesting how pressure might effectively be brought to bear on another part of his own government.

(c) A foreign official acting in unusually close concert with U.S. officials where public knowledge of this might be harmful to that foreign official.

(d) A foreign official whose professional advancement would be beneficial to U.S. interest, especially if any implication has been made of U.S. efforts to further his advancement, or if public knowledge of this might place the person or his career in jeopardy.

(3) All unpublished adverse comments by U.S. officials on the competence, character, attitudes, or activities of a serving foreign government official.

(4) All material that constitutes or reveals unpublished correspondence between heads of state or heads of government.

(5) Statements of U.S. intent to defend, or not defend, identifiable areas, in any foreign country or region.

(6) Statements of U.S. intent to militarily attack identifiable areas in any foreign country or region.

(7) Statements of U.S. policies or initiatives within collective security organizations such as NATO.

(8) Agreements with foreign countries to use, or have access to, military facilities.

(9) Contingency plans as they involve other countries, the use of foreign bases, territory, or airspace; or the use of chemical, biological, or nuclear weapons.

(10) DoD surveys of foreign territories for purposes of basing or using in contingencies.

(11) Statements relating to any use of foreign bases not authorized under bilateral agreements.

(12) Information concerning relationships with foreign intelligence organizations or related to foreign collection activities (see also section 3 of this enclosure which addresses intelligence classification considerations).

c. Classification Guide Illustrations. The discussion on classifying details in Appendix 3 to Enclosure 2 and the recommended format for a security classification guide in Enclosure 4 of this Manual are applicable to DoD development of a foreign relations security classification guide. Subparagraphs 4.c.(1) through 4.c.(3) provide examples of the impact that foreign government information might have on the development of classification guidance.

(1) A DoD Component is involved in negotiating an arrangement with country "X." In the process of the negotiations, the foreign counterpart states that his country does not want discussion on the subject to become public knowledge. At the same time, the foreign official makes it clear that his country has announced publicly its intention to seek U.S. views on the subject of the discussions. The nature of business being discussed is such that the United States would not require the fact of the discussions be protected from public disclosure. Moreover, the subject matter is one that would not ordinarily be classified. The DoD Component, however, does classify the notes and transcripts pertaining to the discussion because of the expressed wishes of the foreign government. The information fits the description of foreign government information. Thus, a classification guide on the subject might contain topics as shown in Table 8 of this enclosure. Remember that use of an exemption (25X1 through 25X9) for the duration of classification as shown in this example requires ISCAP approval prior to use and citation of a declassification date or event (see Enclosure 2, paragraph 2.b for further guidance).

(2) The scenario in paragraph 4.c.(1) and in Table 9 illustrates a brief classification guide involving the foreign relations of the United States as well as foreign government information. The guide could not have been written before negotiations were underway because the foreign official only made the two critical elements of information known during the negotiations. A classification guide such as this one, brief as it is, can serve a very useful purpose when, for example, it is anticipated that the negotiations will involve a large number of personnel from several U.S. agencies and will last several years.

(3) Note that, when previously approved by the ISCAP, exemption 25X9 with a declassification date or event could also be cited for the duration if declassification would violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years. Identify the specific statute, treaty or international agreement in the declassification instructions.

Table 9. Example of Classifying Foreign Government Information Involving Foreign Affairs

CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY

TOPIC	CLASS	REASON	DECLASSIFY ON	REMARKS
1. Apple orchard negotiations with country "X"	U	N/A	N/A	Mere fact of negotiations only; elaboration may be classified, see next topic
2. Transcripts of apple orchard negotiations and substantive notes pertaining to them	C	1.4(b), 1.4(d)	25X6, upon receipt of official approval by country "X" and Dept of State	Requires consultation with foreign government

(4) To illustrate a scenario with military implications, presume that two countries in Europe have secretly granted the United States permission to fly over their territory, but only at high (equal or greater than 50,000 feet) altitudes. One of the countries ("Y") indicated that serious damage would occur to relations if the information became public while the other ("Z") indicated that it did not want the information to be in the public domain. Classification guide topics might read as shown in Table 10. In this example, the guide itself would have to be classified SECRET as it reveals the information that country "Y" has determined would result in serious damage. As in the previous example, exemption 25X9 may also be used if declassification would violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years; specify a declassification date or event, identify the specific statute, treaty or international agreement in the declassification instructions and obtain ISCAP approval prior to using the exemption.

Table 10. Example of Classifying Foreign Government Information with Military Implications

CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY

TOPIC	CLASS	REASON	DECLASSIFY ON	REMARKS
1. Fact of U.S over flights – Europe 1.1 (S) Country "Y" 1.2 (C) Country "Z" 1.3 (U) Other European	 S C U	1.4(d)	25X6, upon receipt of official approval by country "X" and Dept of State	(S) Must be at least 50,000 feet altitude; lower flights not permitted in "Y" and "Z"

ENCLOSURE 4

RECOMMENDED FORMAT FOR A SECURITY CLASSIFICATION GUIDE

1. INTRODUCTION

a. This enclosure discusses and illustrates a general format for a security classification guide. Within the illustrated format, guidance included in brackets ("[ ]") should be replaced with information appropriate for the classification guide under development. Information in parentheses ("( )") provides amplifying information or guidance. Identified sections should be included as appropriate for the needs of the system, plan, program, project, or mission covered by the guide and additional paragraphs or sections may be added if needed to address topics or requirements not covered by the example (e.g., release of information to contractors).

b. Where classification guidance is issued in a form other than a security classification guide (e.g., in a memorandum, plan, order or letter), the document must have enough detail to address all elements of information required by derivative classifiers. The guidance must be approved, in writing, by the OCA.

c. The first interior page of the classification guide may be used as a foreword or introduction, to provide a short synopsis of the technology, system, plan, program, project, or mission covered in the guide. Such information can help potential users quickly understand the content or subjects covered in the security classification guide in more detail than is apparent from the title.

2. COVER PAGE

2. COVER PAGE. The recommended cover page format for a security classification guide includes all of the information shown in Figure 3. If necessary, use an acronym, short title or project number in order to keep title unclassified; place the most significant words of the guide's title first. Mark it "FOR OFFICIAL USE ONLY" or, if classified, with the appropriate classification markings (including classification authority block, portion marks, and any special handling caveats and distribution controls).

Figure 3. Security Classification Guide Cover Page Format

[CLASSIFICATION]

[NAME OF THE SYSTEM, PLAN, PROGRAM, OR PROJECT]

SECURITY CLASSIFICATION GUIDE

[Date]

ISSUED BY: [Name and address of issuing office.]

APPROVED BY: [OCA name and title, or personal identifier.]

[Statement of supersession of previous guides, if any.]

[Distribution Statement for DTIC pursuant to DoDI 5230.24, when required.]

["FOR OFFICIAL USE ONLY" or CLASSIFICATION]

3. CONTENT

a. The actual content of the guide begins with general instructions in section 1 and is followed by specific information on what is to be classified, at what level, and for how long, in sections 2 through 8. Sections 2 through 8 are typically in chart format. Content (interior) pages of the guide must carry the appropriate markings (classification or CUI designation) on each page; see Reference (f) for marking guidance. Insert a page break at the end of each section in the guide. Place the title of the classification guide in capital letter at the top of the first interior page followed by general instructions as illustrated in Figure 4.

Figure 4. Sample Section 1 – General Instructions

[CLASSIFICATION]

[SYSTEM, PLAN, PROGRAM, PROJECT OR MISSION] SECURITY CLASSIFICATION GUIDE

SECTION 1 – GENERAL INSTRUCTIONS

1. Purpose. To provide instructions and guidance on the classification of information involved in [name of the system, plan, program, project, or mission] using an unclassified identification of the effort. (If it is necessary to classify the guide, modify this paragraph as necessary to acknowledge the classified content.)

2. Authority. This guide is issued under authority of [state any applicable departmental or agency regulations authorizing or controlling the issuance of guides, such as DoD Manual 5200.01]. Classification of information involved in [identify the effort] is governed by, and is in accordance with, [cite any applicable classification guidance or guides under which this guide is issued]. This guide constitutes authority and may be cited as the basis for classification, regrading, or declassification of information and material involved in [identify the effort]. Changes in classification required by application of this guide shall be made immediately. Information identified in this guide for protection as classified information is classified by [complete title or position of classifying authority].

3. Office of Primary Responsibility (OPR): This guide is issued by, and all inquiries concerning content and interpretation, as well as any recommendations for changes, should be addressed to:

[Name, code, mailing address of issuing office.] (An administrative or security office in the issuing activity may be used. Inclusion of the action officer's name and phone number/fax and e-mail is recommended.)

4. Classification Challenges. If at any time, any of the security classification guidance contained herein is challenged, the items of information involved shall continue to be protected at the level prescribed by this guide until such time as a final decision is made on the challenge by appropriate authority. Classification challenges should be addressed to the OPR.

5. Reproduction, Extraction, and Dissemination. Authorized recipients of this guide may reproduce, extract, and disseminate the contents of this guide, as necessary, for application by specified groups involved in [identification of the effort], including industrial activities. Copies of separate guides issued to operating activities in application of this guide shall be sent to the OPR. (If it is necessary to classify the guide, modify this paragraph as necessary to express any required limitations.)

[FOR OFFICIAL USE ONLY or CLASSIFICATION]

Figure 4. Sample Section 1 – General Instructions, Continued

[CLASSIFICATION]

6. Public Release. The fact that this guide shows certain details of information to be unclassified, including controlled unclassified information, does not allow automatic public release of this information. DoD information requested by the media or members of the public or proposed for release to the public by DoD civilians or military personnel or their contractors shall be processed in accordance with DoD Manual 5200.01, DoD Directive 5230.09, DoD Instruction 5230.29, and DoD 5400.7-R, as applicable. Proposed public disclosures of unclassified information regarding [identification of effort] shall be processed through [identify office to which requests for public disclosure are to be sent and provide contact information (where the specific office cannot be identified, state that requests should be processed through "appropriate channels for approval")].

7. Foreign Disclosure. Any disclosure to foreign officials of information classified by this guide shall be in accordance with the procedures set forth in [identify applicable issuances implementing DoD foreign disclosure policy, e.g., DoD Directive 5230.11]. If a country with which the DoD has entered into a reciprocal procurement memorandum of understanding or offset arrangement, expresses an interest in this effort, a foreign disclosure review should be conducted prior to issuance of a solicitation. (If it is known that foreign participation cannot be permitted because of the sensitivity of the effort, this fact should be stated. Add other guidance as appropriate.)

8. Definitions. (Include in this paragraph the definitions of any items for which there may be various meanings to ensure common understanding of the details of information that are covered by the guide.)

[FOR OFFICIAL USE ONLY or CLASSIFICATION]

b. Specific information on what is to be classified, at what level, and for how long, is placed in sections 2 through 8, which are typically in table format. Figures 5 through 11 provide descriptions of those sections and Tables 11 through 14 are example charts showing presentation of specific types of information.

(1) The format shown in Tables 11 through 14 is the preferred format, but variations may be used when more appropriate. See the Appendix to this enclosure.

(2) Each table must provide sufficient information to enable the user to fully understand what information is to be protected, at what level, and for how long, so that each derivative document can be properly marked and safeguarded. Use the Remarks column to provide additional information as needed – for example, to provide additional clarification about the information to be classified, to describe the conditions or criteria for each classification within a range of classifications or for alternative classifications, to identify dissemination control markings or special handling caveats, to specify downgrading instructions, to identify another security classification guide that should be consulted for classification guidance for that element of information, or to identify another guide as the original source for the guidance provided.

(3) If data in the table is itself classified, mark the data and table as required by Reference (f).

Figure 5. Sample Section 2 – Overall Effort

SECTION 2 – OVERALL EFFORT

1. Identification. (Include in this paragraph any necessary statements explaining the classifications, if any, to be assigned to various statements identifying the effort. These statements should be consistent with other program documentation.)

2. Goal, Mission, Purpose. (Include in this paragraph any necessary statements identifying information concerning the purpose of the effort that can be released as unclassified and that which must be classified. Take care to ensure that unclassified statements do not reveal classified information.)

3. End Item. (Include in this paragraph statements of the classification to be assigned to the end products of the effort, whether paperwork or hardware. In this connection it is important to distinguish between classification required to protect the fact of the existence of a completed end item, and classification required because of what the end item contains or reveals. In some instances classified information pertaining to performance, manufacture, or composition of incorporated parts or materials is not ascertainable from mere use of or access to the end item. In others, the classifiable information is that which concerns total performance, capabilities, vulnerabilities, or weaknesses of the end item itself, rather than any of the parts or materials.)

Figure 6. Sample Section 3 – Performance and Capabilities

SECTION 3 – PERFORMANCE AND CAPABILITIES

(This section includes characteristics of performance and capability of an end item, or an end item's components, parts, or materials, the performance or capabilities of which require classification. In this section also provide, in sequentially numbered items, statements that express details of performance and capabilities planned and actual. Include both those elements that warrant classification and those that are unclassified. These statements normally would not set forth the numeric values that indicate degree of performance or capability, planned or attained, but merely should identify the specific elements of performance or capability that are covered. When it is necessary to state certain limiting figures above or below which classification is required, the statement itself may warrant classification. For clarity, continuity, or ease of reference it may be desirable to include performance classification data in the sections dealing with the end item or the components or parts to which the performance data apply. Use a "Remarks" column for explanations, limitations, special conditions, associations, etc., as shown in Table 10.)

Table 11. Example of Use of Remarks Column

CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY

TOPIC	CLASSIFCATION	REASON	DECLASSIFY ON	REMARKS
1. Range				
a. Actual	S	1.4(a)	20200615	
b. Predicted	U	N/A	N/A	
2. Accuracy/range rate				
a. Predicted	C	1.4(a)	20200130	
b. Measured	C	1.4(a)	20200130	
3. Altitude				
a. Operational	C	1.4(a)	20200130	
b. Maximum	U or C	1.4(a)	20210130	The general statement "in excess of 50,000 feet" is "U." Otherwise, "C."
4. Commercial Receiver Model No. xxx				
a. Receiver sensitivity, selectivity, and frequency coverage	U	N/A	N/A	Standard commercial receiver characteristics are "U."
b. Fact of application or use in this effort	S	1.4(a)	20250415	
5. Resolution, Thermal				
a. Maximum attainable	U or S	1.4(a)	20210415	Planned or actual attained thermal resolutions above 0.25 degrees C are "U." Otherwise, "S."
b. Operational optimum	U or S	1.4(a)	20210415	Planned or actual attained thermal resolutions above 0.25 degrees C are "U." Otherwise, "S//REL TO USA, GBR"
c. Operational attainment	U or S	1.4(a)	20210415	Planned or actual attained thermal resolutions above 0.25 degrees C are "U." Otherwise, "S//REL TO USA, GBR"
6. Speed				Generic reference to "supersonic" speed is "U."
a. Maximum	S	1.4(a)	20210115	Downgrade to "C" upon IOC.
b. Rate of climb	S	1.4(a)	20210115	Downgrade to "C" upon IOC.
c. Intercept	S	1.4(a)	20210115	Downgrade to "C" upon IOC.

Figure 7. Sample Section 4 – Specifications

SECTION 4 – SPECIFICATIONS

This section includes items of information describing standards for [qualities of materials and parts; methods or modes or construction, manufacture or assembly; and specific dimensions in size, form, shape, and weight, that require classification]. Inclusion in this section is required because the items require classification because they contribute to the national security advantage resulting from this effort, or because they frequently require classification but are unclassified in [identification of this effort]. Classification of specifications pertaining to performance and capability are covered in section 3 of the guide. (Actual figures do not need to be given, merely statements identifying clearly the specific items of information involved. If figures are necessary to establish classification levels, it may be necessary to classify the statements themselves. When necessary for clarity, continuity or ease of reference, specification classification data may be included in sections on the end product or components or parts to which the data apply. Use a "Remarks" column for explanations, limitations, special conditions, associations, etc.)

Table 12. Example of Specifications

CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY

TOPIC	CLASS	REASON	DECLASSIFY ON	REMARKS
1. Burn rate	C	1.4(a)	20210917	
2. Power requirement	U or S	1.4(a)	20210917	"S" when associated with Model No. #. Otherwise "U."
3. Chemical composition	U	N/A	N/A	Composition is FOUO

Figure 8. Sample Section 5 – Critical Elements

SECTION 5 – CRITICAL ELEMENTS

(This section is used only if there are specific elements that are both critical to the successful operation of the end item of this effort and unique enough to warrant classification of some data concerning them. Provide in sequentially numbered paragraphs each significant items of information peculiar to these critical elements and the classification applicable. Also include in this section the classification to be assigned to information pertaining to components, parts, and materials that are peculiar and critical to the successful operation of the end item in this effort when such items of information are the reason for or contribute to the national security advantage resulting from this effort. Performance data pertaining to such critical elements can be included in this section instead of section 3 of the guide.)

Figure 9. Sample Section 6 – Vulnerabilities and Weaknesses

SECTION 6 – VULNERABILITIES AND WEAKNESSES

(This section is used to specify classification to be assigned to details of information that disclose inherent weaknesses that could be exploited to defeat or minimize the effectiveness of the end product of this effort. Classification assigned to details of information on countermeasures and counter-countermeasures should also be included in this section.)

Figure 10. Sample Section 7 – Administrative Data

SECTION 7 – ADMINISTRATIVE DATA

(This section is used only if particular elements of administrative data, such as program information, procurement schedules, production quantities, schedules, programs, or status of the effort, and data on shipments, deployment, or transportation and manuals (field, training, etc.), warrant classification. Table 12 provides examples of possible classified administrative data.)

Table 13. Example Showing Classified Administrative Data

CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY

TOPIC	CLASS	REASON	DECLASSIFY ON	REMARKS
1. Budget data				
a. FY budget total	U	N/A	N/A	
b. Budget estimate data, including total	U	N/A	N/A	"FOUO" prior to White House /OMB release to Congress.
2. Programmed end item production rate	U	N/A	N/A	"FOUO" prior to contract award.
3. Planned delivery mode	U	N/A	N/A	
4. Planned equipment delivery rate	C	1.4(a)	20300313	
5. Actual routing of delivery of end items	C	1.4(a)	See remarks, but not later than (NLT) 20300313	Classify upon selection of route, and declassify upon completion of last delivery to site.
6. Scheduled shipping dates and times	C	1.4(a)	See remarks, but NLT 20300313	Classify upon decision to ship, and declassify upon off-load at destination.

Figure 11. Sample Section 8 – Hardware

SECTION 8 – HARDWARE

(Table 13 provides an example of classification of hardware items. The degree of specificity to be included in this section will depend largely upon:

a. The level from which issued. When issued from a headquarters level, the classification is most likely to be applied to the hardware end item itself, rather than its individual components.

b. The channels or hands through which the guidance will travel to the ultimate user. The closer the issuer is to the user, the more detailed the guidance may become. When the issuer is removed from the user, intermediate levels of guidance may be required to expand or elaborate on the guidance provided by the basic classification guide and to cover more details concerning materials, parts, components, assemblies, and subassemblies, and the classification, if any, to be assigned. Any such expansion or elaboration should be fully coordinated with the headquarters issuing the basic guide.

c. The ease of determining when classified information could be revealed by a particular hardware item. Obscure connections and associations that could reveal classified information may require the issuer of the guide to state classification for certain hardware items. In such cases it probably would be advisable to explain why classification is necessary.

d. Whether there are factors that require consideration and action at a headquarters level. National or DoD policy, intelligence data, broad operational requirements, extraneous factors, or other matters not ordinarily available below headquarters, or that require high level consideration may result in decisions to classify certain hardware items.)

Table 14. Example Showing Hardware Classification

CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY

TOPIC	CLASS	REASON	DECLASSIFY ON	REMARKS
1. End item hardware:				
a. AN/APR-999	C	1.4(a)	20200820	External views of the assembled AN/APR-999 are "U."
(1) Analyzer unit	C	1.4(a)	20200820	
(2) Threat display unit	U	N/A	N/A	Display specifications are FOUO.
(3) Preamplifier	U	N/A	N/A	
b. AN/APR-0000	U	N/A	N/A	

APPENDIX TO ENCLOSURE 4

FORMAT VARIATIONS

Use of the standard format as described and illustrated in the other enclosures of this Manual is strongly recommended as it provides a consistent Department-wide structure and facilitates understanding and use of other security classification guides when looking for information. However, in some instances other headers and formats are more advantageous and efficient for the users. Figures 12 through 15 illustrate column headers and arrangements that are different from those used in Enclosure 4. These headers and arrangements may be employed in the construction of a classification guide and may additionally be modified to suit the needs of the specific effort. For example, a column for downgrading action could be added if most items of information have downgrading instructions assigned, but such a column would not be necessary if the guide did not provide downgrading instructions or if only one or two items of information are to be downgraded. In the later case, the downgrading instruction could be placed in the "Remarks" column.

Figure 12. Format Variation 1

TOPIC	CLASSIFICATION	REASON	DURATION	REMARKS

Figure 13. Format Variation 2

DESCRIPTION	CLASSIFICATION	REASON	DECLASSIFY UPON	DISSEMINATION/ SPECIALHANDLING	REMARKS

Figure 14. Format Variation 3

INFORMATION REVEALING	CLASSIFICATION/ DECLASSIFICATION	REASON	REMARKS

Figure 15. Format Variation 4

REASON: All information in this section is classified per section 1.4(_) of E.O. 13526		
TOPIC	**CLASSIFICATION**	**DECLASSIFY ON**

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

C	Confidential
CFR	Code of Federal Regulations
COMSEC	communications security
CUI	controlled unclassified information
DASD(NM)	Deputy Assistant Secretary of Defense for Nuclear Matters
DoDD	DoD Directive
DoDI	DoD Instruction
DOE	Department of Energy
DTIC	Defense Technical Information Center
E.O.	Executive Order
FOUO	For Official Use Only
FRD	Formerly Restricted Data
HUMINT	human intelligence
IOC	initial operational capability
IR&D	independent research and development
ISCAP	Interagency Security Classification Appeals Panel
N/A	not applicable
NATO	North Atlantic Treaty Organization
NLT	not later than
NOFORN	Not Releasable to Foreign Nationals
NSI	national security information
OCA	original classification authority
OPR	office of primary responsibility
OPSEC	operations security
RD	Restricted Data
REL TO	Releasable To
S	Secret
TS	Top Secret
U	Unclassified
U.S.C.	United States Code
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Manual.

downgrading. A determination by an OCA or declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

FRD. Information removed from the RD category upon a joint determination by DOE (or antecedent agencies) and DoD that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. FRD is treated the same as RD for purposes of foreign dissemination.

fundamental research. Basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

horizontal classification. Classification of information associated with more than one system, plan, program, project, or mission at the same level by all involved activities and organizations.

IR&D. Research and development effort that is neither sponsored by a grant, nor required in performing a contract, and which falls under any of the following four areas:

Applied research.

Basic research.

Development.

Systems and other concept formulation studies.

military operations information. Information pertaining to a strategic or tactical military action, including training, movement of troops and equipment, supplies, and other information vital to the success of any battle or campaign.

NSI. Information that has been determined, pursuant to Reference (d), or any predecessor order, to require protection against unauthorized disclosure.

OCA. An individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to originally classify information (i.e., to classify information in the first instance). Reference (f) provides guidance on designation of OCAs.

RD. All data concerning design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but not data declassified or removed from the RD category pursuant to section 2162 of the Atomic Energy Act of 1954, as amended.